

# Multiparty Quantum Private Comparison with Individually Dishonest Third Parties for Strangers

Shih-Min Hung, Sheng-Liang Hwang, Tzonelih Hwang, and Shih-Hung Kao

July 26, 2016

## Abstract

This study explores a new security problem existing in various state-of-the-art quantum private comparison (QPC) protocols, where a malicious third-party (TP) announces fake comparison (or intermediate) results. In this case, the participants could eventually be led to a wrong direction and the QPC will become fraudulent. In order to resolve this problem, a new level of trustworthiness for TP is defined and a new QPC protocol is proposed, where a second TP is introduced to monitor the first one. Once a TP announces a fake comparison (or intermediate) result, participants can detect the fraud immediately. Besides, due to the introduction of the second TP, the proposed protocol allows strangers to compare their secrets privately, whereas the state-of-the-art QPCs require the involved clients to know each other before running the protocol.

**Keywords:** Quantum cryptography; Quantum private comparison; Third-party; Semi-honest; Almost dishonest; Individually dishonest; The stranger environment

# 1 Introduction

Quantum private comparison (QPC) is an imperative branch of secure multi-party computing, which allows participants to determine whether their secrets are equal or not without revealing their secrets. The first QPC protocol was proposed by Yang et al. [1] using Einstein–Podolsky–Rosen (EPR) pairs. The security in Yang et al.’s protocol is based on the use of decoy photons in the quantum transmission and the one-way hash function for protection the secrets of the participants. However, since the round trip quantum transmissions are adopted in Yang et al.’s protocol, special optical filters are required to prevent Trojan horse attack [2–4], which decreases the qubit efficiency. Accordingly, in order to enhance the qubit efficiency, Chen et al. [5] proposed a QPC protocol using a triplet Greenberger-Horne-Zeilinger (GHZ) states. Since then, many QPC protocols [6–11] have been proposed based on various quantum entangled states. For example, Tseng et al. [11] proposed a QPC protocol without any entangled EPR pairs and other QPC protocols such as in [6–10] use the EPR pairs, GHZ states, triplet W states and the  $\chi$ -type genuine four particle entangled states for private information comparison.

The protocols described above can only compare the secrets for just two participants. Until 2013, the first multiparty QPC protocol with GHZ state was proposed by Chang et al. [12], in which  $n$  participants can compare whether the private information of any two users is equal or not. Then Liu et al. [13] proposed a multiparty QPC protocol using d-dimensional basis state. Hereafter, many multiparty QPC protocols have been proposed. Most of them also use the GHZ state or d-dimensional basis state. Here, our proposed protocol is based on the GHZ state.

All the QPC protocols proposed so far require a third-party (TP) to help the participants compare their secrets, generate photons and announce the com-

parison (or intermediate) result. In this regard, four types of QPCs can be categorized based on the levels of **trustworthiness of the TP** [14].

1. First, TP is considered as an **honest** agent. Since the participants can trust TP, they just send their secrets to TP for comparison. This situation is an ideal one, but in reality, the assumption of an honest TP is very unrealistic.
2. Next, TP is considered as a **semi-honest** agent, where both participants can trust TP partially. In this case, TP will loyally execute the protocol, but may try to steal participants' secret using passive attacks. The semi-honest TP will passively collect the classical information exchanged between participants and try to reveal their secrets from this information.
3. Then, TP is considered as an **almost dishonest** agent, where both participants can also trust TP partially. In this case, TP may try to steal the information by modifying the procedure of the protocol actively. However, it cannot collude with other participants. The collude behavior includes the following cases:
  - (1) People works together to do something bad.
  - (2) A person helps the other person to avoid the detection if he/she knows the other one is attacking.
  - (3) A person executes the protocol dependently with the other, which should be independently in the protocol.

It means TP will not help any attacker steal the secrets of participants. In other words, the TP not only can passively collect useful information but also can actively perform any attack on the protocol except conspiring with the participant. In some papers, this type of TP is also named as semi-honest TP, a term easily confusing with the definition in 2.

4. Finally, TP is considered as a dishonest agent, where both the participants cannot trust TP. This situation is the same as the two party QPC protocol without TP, which has been proven to be insecure by Lo et al. [15].

### 1.1 Problem Statement and Motivation

So far, we know that a TP plays a major role in many QPC protocols. Even though several levels of trustworthiness of TP have been defined, many recent QPC protocols adopt the assumption of an almost dishonest TP, which unfortunately did not mention anything about whether or not the TP will always announce a correct comparison (or intermediate) result. However, if the TP announces a fake result, then all of above protocols will be incorrect because the participants are not able to detect this fraud. For example, if two participants are bidding and comparing their prices, then the TP will announce a fake result to disturb their bidding process, even if he/she cannot obtain useful information and benefits. Hence, it is necessary for us to define a new level of trustworthiness for this type of TP. Here, this particular type of TP is called “**individually dishonest TP**,” who could independently act maliciously. The definition of individually dishonest TP is that the TP may announce a fake result or try to actively steal the information by modifying the procedure of the protocol except conspiring with participants or other TPs.

Hence, how to detect and prevent this individually dishonest TP’s malicious behavior is a challenging problem. The entire levels of trustworthiness of TP can also be shown in Fig. 1, where except the inner-most layer, each layer higher automatically assumes the capability of the layer inner.

According to the above figure, the individually dishonest is more close to dishonest and hence is more practical, where except for the conspiring attack, the TP can perform “any” possible attack – including the denial-of-service attack

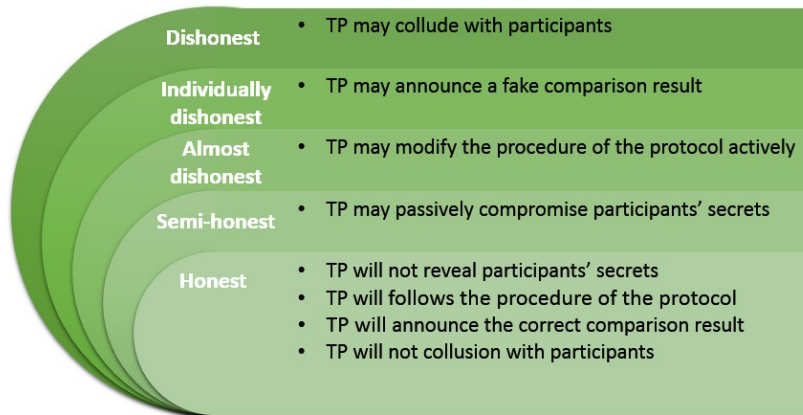


Figure 1: Level of trustworthiness of TP

– and the QPC protocol can still be secure.

Furthermore, this article also investigates a new environment, called the stranger environment, where participants could be strangers. As contrary of this scenario, the state-of-the-art QPC protocols assume the existence of authentication channels or pre-sharing keys between participants in order to check the initial state or prevent private information from leakage. The authentication channel allows the receiver to conform the integrity of the transmitted message and the originality of the sender, but the transmitted classical message is public. However, sharing authentication channels or keys between the participants requires them to establish some relationship beforehand. Can we construct a QPC protocol for strangers who do not pre-share any key or quantum states? To summarize our discussion, in this paper we intend to propose a new multiparty QPC protocol with GHZ states, which is resilient to the individually dishonest TPs in a stranger environment.

In the following, we will consider Zhang et al.’s protocol [14] as an example to show the problems with an individually dishonest TP. Subsequently, a new QPC protocol will be proposed with detailed security analysis.

The rest of this paper is organized as follows. Section 2 reviews Zhang et al.’s protocol and describes the problems. Section 3 gives a solution protocol with individually dishonest TP for strangers. Section 4 analyzes the security of the proposed protocol. Finally, a concluding remark is given in Section 5.

## 2 Zhang et al.’s protocol and Problems

Let Alice and Bob be two participants, who want to compare the equality of their  $m$ -bit secret information  $M_A$  and  $M_B$  via the help of an almost dishonest TP without leaking any private information to the TP or any outsider. Zhang et al.’s protocol proceeds in the following steps:

**Step1** TP prepares  $m$  EPR pairs randomly chosen from two Bell states  $|\phi^+\rangle$ ,  $|\psi^-\rangle$ , where  $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ,  $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ . TP divides these EPR pairs into two sequences  $S_A$  and  $S_B$ , representing sequences of all the first photons and all the second photons respectively.

**Step2** Step 2. TP prepares two sets of decoy photons  $D_A$  and  $D_B$  randomly chosen from  $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ,  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ . Each set contains  $m$  qubits. TP randomly inserts  $D_A$  to  $S_A$  (and  $D_B$  to  $S_B$ ) to form a new sequence  $S_A^*$  (and  $S_B^*$ ), and then sends  $S_A^*$  and  $S_B^*$  to Alice and Bob, respectively.

**Step3** After Alice (Bob) receives  $S_A^*$  ( $S_B^*$ ), she (he) and TP perform public discussion to check eavesdroppers.

**Step4** After the public discussion, Alice and Bob can share many Bell states and TP is the only one who knows the initial state of these Bell states. Then, Alice, Bob and TP work together to check the correctness of the states.

**Step5** Step 5. Alice (Bob) uses Z-basis to measure the photons in  $S_A$  ( $S_B$ ). If the measurement result is  $|0\rangle$ , then Alice (Bob) encodes it as the classical bit '0'; if the measurement result is  $|1\rangle$ , then Alice (Bob) encodes it as the classical bit '1.' Hence, Alice (Bob) obtains a key bit string  $K_A$  ( $K_B$ ).

**Step6** Alice (Bob) calculates the comparison information  $C_A = K_A \oplus M_A$  ( $C_B = K_B \oplus M_B$ ), where  $\oplus$  is a bitwise exclusive-OR operation. They also collaborate together to compute the comparison information  $C = C_A \oplus C_B$  and send  $C$  to TP.

**Step7** After TP gets  $C$  from Alice and Bob, TP transforms the initial Bell state ( $S_A, S_B$ ) into a classical bit string  $C_T$  and calculates the comparison

result  $R = C_T \oplus C$ . If there is a ‘1’ in  $R$ , then TP terminates the protocol and announces the result that the two participants’ secret information is different. Otherwise, (i.e., if all bits in  $R$  are ‘0’), TP announces the result that the two participants’ secret information is identical.

Within the protocol, if the TP announces a fake comparison result, then according to Step 7, the participants cannot detect it. Hence, the participants can do nothing but accept the wrong comparison result. Besides, in Step 4, since the participants have to communicate with each other to check the integrity of the almost dishonest TP so as to avoid TP’s manipulation of their communication, they require to establish an authentication channel between them. However, in a stranger environment, where both clients could be strangers and hence do not share an authentication channel between them, this protocol cannot be applicable. The same problems can also be found in the other state-of-the-art QPC protocols such as in [1, 5–14].

### 3 The proposed scheme

A multiparty QPC protocol for strangers with two individually dishonest TPs is proposed here. Let  $TP_1, TP_2$  be two individually dishonest TPs. According to the previous definition, the individually dishonest TPs may announce a fake comparison (or intermediate) result to participants, though they cannot collude with each other or with the participants. By the help of both TPs, participants can detect whether any TP announces a wrong result. Besides, participants involved in the protocol could be strangers, i.e., they do not need to pre-share any secret or establish any authentication channel directly for communication before-hand among them. In this protocol, there are quantum channels and authentication channels between TPs and between each TP and each participant. There are only classical channels between participants.



In this section, the GHZ states used in the protocol are first reviewed in Section 3.1. The detail description of the proposed multiparty QPC protocol is given in Section 3.2. The usefulness of the proposed protocol in the stranger environment is described in Section 3.3. Finally, the discussion about the malicious TP will be given in Section 3.4.

### 3.1 The property of GHZ state

The GHZ states are as follows:

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}} \left( |q_1, q_2, \dots, q_n\rangle + (-1)^\Delta |\overline{q_1, q_2, \dots, q_n}\rangle \right),$$

where  $i = 1, 2, 3, \dots, 2^n$ ,  $q_1 = 0$ ,  $q_2, q_3, \dots, q_n \in \{0, 1\}$ ,  $\Delta = i - 1 \pmod{2}$  and  $n$  denotes the number of participants.

The above state can also be re-written in X basis,  $\{|+\rangle, |-\rangle\}$ , which is as follows:

$$|\Psi_i\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{n(-)=\text{odd/even}} (-1)^\delta |x_1, x_2, \dots, x_n\rangle,$$

where  $x_i \in \{+, -\}$  satisfies the condition of  $n(-)$ , the number of  $-$  in  $x_1, x_2, \dots, x_n$ .

If  $\Delta = 0$ , then  $n(-)$  will be even; otherwise, if  $\Delta = 1$ , then  $n(-)$  will be odd.

$$\delta = \bigoplus_{\{i|x_i=-\}}.$$

For example, a three-qubit GHZ state  $|\Psi_5\rangle = \frac{1}{\sqrt{2}} (|010\rangle + |101\rangle)$  can be written in X-basis as follows:

$$\begin{aligned} |\Psi_5\rangle &= \frac{1}{\sqrt{2^{3-1}}} \sum_{\text{even}} \left[ (-1)^\delta |x_1, x_2, \dots, x_n\rangle \right] \\ &= \frac{1}{2} \left[ (-1)^0 |+++ \rangle + (-1)^{1\oplus 0} |+- - \rangle + (-1)^{0\oplus 0} |-+ - \rangle + (-1)^{0\oplus 1} |--+ \rangle \right] \\ &= \frac{1}{2} (|+++ \rangle - |+- - \rangle + |-+ - \rangle - |--+ \rangle). \end{aligned}$$

According to Heisenberg uncertainty principle, the measurement result of the  $i$ -th particle could be either  $|q_i\rangle$  or  $|\overline{q_i}\rangle$  with a probability of 50%. Hence,

no one can predict the measurement result of the  $i$ -th particle. However, for a particular GHZ state  $|\Psi_w\rangle$ , where  $1 \leq w \leq 2^n$ , if we measure two arbitrary particles, e.g., the  $i$ -th particle and the  $j$ -th particle, and obtain the measurement  $m_i$  and  $m_j$  respectively, then the xoring value  $m_i \oplus m_j$  is fixed. For example, let  $n = 4$  and  $w = 7$ , if the initial state is  $|\Psi_7\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$ , then the xoring value of first particle and second particle is always '0' and the xoring value of second particle and fourth particle is always '1'. Hence, if one knows the initial state of a GHZ state, he can infer the xoring value of measurement results of two arbitrarily particles. In the following, TPs will utilize this property to do the comparison between each pair of users.

### 3.2 Proposed Multiparty QPC protocol

Let  $P_1, P_2, \dots, P_n$  denote  $n$  participants, who want to compare the equality of their  $m$ -bit secret information  $M_1, M_2, \dots, M_n$  via the help of two individually dishonest TPs,  $TP_1$  and  $TP_2$ , without leaking any private information to the TPs or any outsider. The proposed protocol proceeds in the following steps: (as also described in Fig. 2)

**Step1**  $TP_1$  randomly prepares  $2m$   $n$ -particle GHZ states as described in Section 3.1.  $TP_1$  divides these GHZ states into  $n$  sequences  $S_i$ , where  $1 \leq i \leq n$ , representing sequences of all the  $i$ -th photons in these  $2m$  initial states, respectively.

**Step2**  $TP_1$  prepares  $n$  sets of decoy photon  $D_1, D_2, \dots, D_n$  randomly chosen from  $|0\rangle, |1\rangle, |+\rangle$ , and  $|-\rangle$ . Each set contains  $2m$  qubits.  $TP_1$  randomly inserts  $D_1 (D_2, \dots, D_n)$  into  $S_1 (S_2, \dots, S_n)$  respectively to form the new sequence  $S_1^* (S_2^*, \dots, S_n^*)$  and sends  $S_i^*$  to  $P_i$  respectively. After  $P_i$  receives  $S_i^*$ , he/she and perform the public discussion to check the existence of eavesdroppers. First,  $TP_1$  announces the positions and bases

of decoy photons  $D_i$ . Then,  $P_i$  will divide  $S_i^*$  into  $S_i$  and  $D_i$  by the positions and use correct basis to measure the corresponding decoy photon. Hereafter, the participants send back the measurement results to  $TP_1$ . Finally,  $TP_1$  checks the existence of eavesdroppers by checking whether the measurement results are correct or not. If they are correct, the protocol can be continued. Otherwise, the protocol will be aborted. Then,  $TP_1$  sends the information of the initial GHZ states to  $TP_2$  using quantum secure direct communication protocol, e.g., [16].

**Step3** After the public discussion,  $P_1, P_2, \dots, P_n$  can share many GHZ states and  $TP_1$  and  $TP_2$  are the only two who know the initial states of these GHZ states. Then, all participants and  $TP_2$  work together to check the correctness of the states. For example, (1)  $P_1$  randomly chooses the particles for checking and announces the positions of those particles. (2)  $P_2$  randomly selects either Z-basis or X-basis for each chosen particle and announces the bases. (3) All participants use the selected bases to measure the corresponding particles and subsequently broadcast their measurement results for each chosen particle. (4)  $TP_2$  checks the measurement results and the initial state sent from  $TP_1$  and announces whether or not the measurement results correspond with the initial states, which should satisfy the equations described in Section 3.1. If yes, then it implies that there is no eavesdropper and  $TP_1$  prepares the initial state loyally and also the information of initial state sent from  $TP_1$  is correct. Otherwise, they abort this protocol.

**Step4**  $P_i$  uses Z-basis to measure the photons in  $S_i$  and obtains a key string of measurement result  $K_i$ . That is, if the measurement result is  $|0\rangle$ , then  $P_1$  encodes it as the classical bit '0'. If the measurement result is  $|1\rangle$ , then  $P_1$  encodes it as the classical bit '1'. calculates the comparison information

$$C_i = K_i \oplus M_i.$$

**Step5**  $P_i$  sends  $C_i$  to  $TP_1$  and  $TP_2$  via authenticated channels.

**Step6** After  $TP_1$  gets  $C_i$ 's from all participants, for arbitrary two participants,  $P_i$  and  $P_j$ ,  $TP_1$  calculates the comparison result  $R_{ij} = T_{ij} \oplus C_i \oplus C_j$ , respectively, where  $T_{ij}$  is the expected xoring value of the  $i$ -th and  $j$ -th particles in that particular GHZ state. If there is a '1' in  $R_{ij}$ , then  $TP_1$  announces that the secret information of  $P_i$  and  $P_j$  is different. Otherwise,  $TP_1$  announces that the secret information of  $P_i$  and  $P_j$  is identical. Similarly,  $TP_2$  also does the comparison and announces the comparison result, too.

**Step7** Any two participants,  $P_i$  and  $P_j$ , can compare the  $R_{ij}$  between  $TP_1$  and  $TP_2$ . If the results are the same, then they believe both  $TP_1$  and  $TP_2$  announce the correct result. Otherwise, they know that one of TPs announce a wrong result and the entire comparison process will be aborted.

The correctness of this protocol is based on the property of GHZ state described in Section 3.1. Since we know the xoring value,  $T_{ij} = K_i \oplus K_j$ , of the  $i$ -th and the  $j$ -th particles in a particular GHZ state, we can calculate that  $R_{ij} = T_{ij} \oplus C_i \oplus C_j = T_{ij} \oplus K_i \oplus K_j \oplus M_i \oplus M_j = M_i \oplus M_j$ . Hence, if all bits in  $R_{ij}$  are '0', it means all bits in  $M_i$  and  $M_j$  are equal and the secret information of  $P_i$  and  $P_j$  is identical.

### 3.3 Stranger environment

This protocol also can work on a stranger environment because the involved users are communicating only on classical channels. In Step 3, in order to prevent from  $TP_1$ 's attacks, all participants are communicating on classical channels, even though the communication between each user and  $TP_2$  will

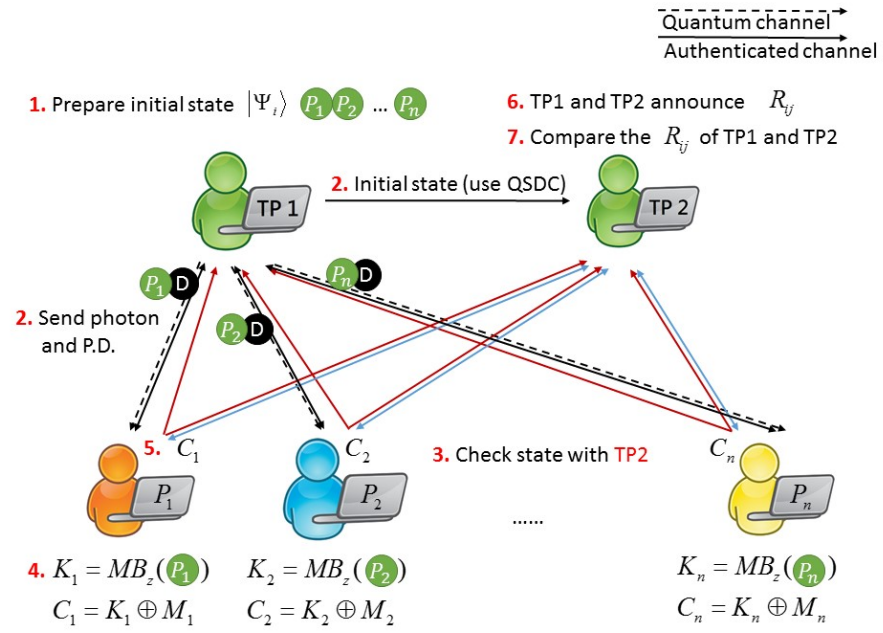


Figure 2: Proposed multiparty QPC protocol

eventually detect it. For example, in Step 3,  $P_1$  randomly chooses the particles for checking and announces the positions of those particles to the other participants via classical channels. Now, if the information in the classical channel is modified by an outsider, then the other participants will receive wrong positions. In that case, they all measure the wrong photons except  $P_1$ . Since the measurement results may not correspond with the initial state with a high probability,  $TP_2$  will detect this fraud. For instance, suppose that the initial state of a particular chosen position,  $i$  ( $1 \leq i \leq m$ ), is  $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{2}(|+++\rangle + |+-\rangle + |-+-\rangle + |--+\rangle)$ . If the correct photons in the state are measured, then the measurement result will be  $|000\rangle$  or  $|111\rangle$  in Z-basis and  $|+++\rangle$ ,  $|+-\rangle$ ,  $|-+-\rangle$ , or  $|--+\rangle$  in X-basis. However, if the checking position has been modified by an outsider to the other position  $j$  ( $1 \leq j \leq m$ ) with the initial state  $|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle) = \frac{1}{2}(|+++\rangle + |+-\rangle + |-+-\rangle + |--+\rangle)$ , then measures the photon in  $i$ , whereas the others will measure the photons in  $j$ . Consequently the measurement result obtained by  $TP_2$  will become  $|100\rangle$ ,  $|011\rangle$ ,  $|000\rangle$ , or  $|111\rangle$  in Z-basis and  $|+++\rangle$ ,  $|+-\rangle$ ,  $|-+-\rangle$ ,  $|--+\rangle$ ,  $|-++\rangle$ ,  $|--+\rangle$ ,  $|++-\rangle$ , or  $|+-+\rangle$  in X-basis which will correspond to  $|\Psi_1\rangle$  with a probability of 50%. Hence, for  $l$  initial states, the detection rate is  $1 - (1/2)^l$  which is close to 1 if  $l$  is large enough.

Since there are only classical channels between participants, there may be DOS attack in Step 3 if the classical channels are frequently disturbed. However, with a little modification, this sort of DOS attack can be prevented. The modification is as follows. Instead of announcing the positions of the chosen particles via classical channels,  $P_1$  informs  $TP_2$  the positions of the chosen particles via the authentication channel, and  $TP_2$  informs all the other participants that information also via authentication channels. Similarly  $P_2$  announces the

information via authentication channels in Step 3, too. With this modification, no classical channel is used and hence the DOS attacker cannot be successful.

### 3.4 Who is telling a lie

As mentioned earlier that an individually dishonest TP could announce a fake comparison result. However, since the other TP also does the same comparison and announces the comparison result, participants will eventually detect the inconsistency if one of the TPs is not honest. Unfortunately, the current protocol cannot identify which TP announced the fake comparison result. To identify the dishonest TP, an arbitrated quantum signature protocol, e.g., [17] can be introduced to the proposed scheme with the help of a trusted arbitrator as follows. In Step 2, instead of sending the information of the initial GHZ states to  $TP_2$ ,  $TP_1$  signs the information of the initial states via an arbitrated quantum signature for  $TP_2$  and protects the privacy of the content by using the keys between TPs and arbitrator. Later, this information can be used by the arbitrator to identify the TP who was telling a lie, because the arbitrator can use the signed initial states to do the comparison and hence can identify the dishonest TP.

## 4 Security Analysis

In this section, we show that our proposed protocol has several imperative security properties, which are important for a secure QPC protocol. This section contains two parts, the outsider attack (Section 4.1), the insider attack (Section 4.2).

## 4.1 Outsider attack

After  $TP_1$  sends all photons to each participant, all participants and  $TP_1$  perform public discussion to check outsider attack. First,  $TP_1$  announces the positions and bases of all decoy photons. Later, each participant gets the measurement results by measuring the corresponding decoy photons. Then, every participant sends back the measurement results to  $TP_1$ .  $TP_1$  checks the existence of eavesdroppers by checking whether the measurement results are correct or not.

Since the eavesdropper, Eve, does not know the positions and measurement bases of the decoy photons, some well-known attacks such as intercept-resend attack [18], correlation-elicitation attack [19], and entanglement-measure attack [20] can be detected via the checking mechanism [3]. For example, if Eve measures the decoy photon  $|0\rangle$  or  $|1\rangle$  with Z-basis  $\{|0\rangle, |1\rangle\}$ , she will pass the public discussion. However, if Eve measures the decoy photon  $|0\rangle$  or  $|1\rangle$  with X-basis  $\{|+\rangle, |-\rangle\}$ , because of the quantum property, the probability that she will be detected is 50%. Obviously, the probability that Eve chooses the wrong measurement basis is 50%. Therefore, the detection rate for each decoy photons is 25% ( $50\% \times 50\%$ ). For  $l$  decoy photons (where  $l$  is large enough), the detection rate is  $1 - (3/4)^l$  which is close to 1 if  $l$  is large enough. Furthermore, since quantum bits are transmitted only once in the proposed protocol, the Trojan horse attack can be automatically prevented. Therefore, the proposed protocol is free from any outsider attack.

## 4.2 Insider attack

In this sub-section, three cases of insider attack will be considered. The first case discusses about the participants' attack. The second and third cases discuss the attack from  $TP_1$  and  $TP_2$ , respectively.



### Case 1. Participants' attack

Suppose that Alice attempts to reveal Bob's secret.  $TP_1$  and  $TP_2$  are individually dishonest TPs who will not conspire with each other and with the participants. In this case, if Alice tries to intercept the transmitted photon from  $TP_1$  to Bob, she will be caught as an eavesdropper as discussed in Section 4.1. Therefore, the only possible way for Alice to obtain Bob's private information is using her photon to extract Bob's measurement result. If Alice knows the initial state, she could calculate Bob's measurement result by the measurement result of Alice's photon and the initial state. For example, suppose the initial state is  $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{2}(|+++\rangle + |+-\rangle + |-+-\rangle + |--+\rangle)$ . If the measurement result of Alice  $K_A$  is 0, then she will know the measurement result of Bob's  $K_B$  is also 0. By knowing  $K_B$  and  $C_B$ , Alice can calculate the secret information of Bob's  $M_B$ . However, since Alice does not know anything about the initial state, it is impossible for her to perform this attack.

### Case 2. $TP_1$ 's attack

In the proposed protocol, the responsibility of  $TP_1$  is to generate initial states, inform  $TP_2$  the initial states and compare the private information.  $TP_1$  may try to steal participants' secrets by using fake initial states instead of the official initial states. However, in Step 3,  $TP_2$  and all the participants work together to check the correctness of the initial states, so if  $TP_1$  use a fake initial state, he will be caught. For example, suppose there are three participants.  $TP_1$  generates  $|000\rangle$  as the initial state and sends those particles to three participants respectively as in Step 2, but  $TP_1$  tells  $TP_2$  a lie about the initial state as  $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{2}(|+++\rangle + |+-\rangle + |-+-\rangle + |--+\rangle)$ . All participants use Z-basis to measure the photon and get the key bit  $K_i$ . Since  $TP_1$  knows that the photons all participants received are  $|0\rangle$ , he/she will know

the key bits  $K_1$  for each participants is '0'. Then, each participant  $P_i$  sends  $C_i$  to  $TP_1$ . As the result,  $TP_1$  can easily calculate participants' secrets  $M_i$ . However, this attack of  $TP_1$  will be detected in Step 3, because if the participant  $P_2$  chooses X-basis to check, then the measurement results will not always be in  $\{|+++\rangle, |+- -\rangle, |-+-\rangle, |--+\rangle\}$  and hence the fake initial state of  $TP_1$  will be detected.

### Case 2. $TP_2$ 's attack

In the proposed protocol, the responsibility of  $TP_2$  is to check the correctness of the initial states and compare the private information of each pair of users.  $TP_2$  may try to steal participants' secrets by intercepting the transmitted photons from  $TP_1$  to participants. However,  $TP_2$  will be caught in the eavesdropper detection discussed in Section 4.1.

## 5 Conclusion

A new security problem about the trustworthiness of a TP, who could announce a fake comparison result, in the state-of-the-art QPC protocols is identified, which may cause the participants to believe in a wrong comparison result. To explore further the problem, a new TP named individually dishonest TP, is defined. Subsequently, a multiparty QPC protocol, which provides a solution to detect the fake comparison (or intermediate) result announced by a TP has been proposed. We argue that the proposed protocol can also work in a stranger environment, where there is no authentication channel or no pre-shared key between each pair of participants. Moreover, the proposed protocol has been shown to be secure against both the outsider and the insider attacks.

## Acknowledgment

We would like to thank the Ministry of Science and Technology of Republic of China for financial support of this research under Contract No. MOST 104-2221-E-006-102 -.

## References

## References

- [1] Y.-G. Yang and Q.-Y. Wen, “An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement,” *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 5, p. 055305, 2009. [Online]. Available: <http://stacks.iop.org/1751-8121/42/i=5/a=055305>
- [2] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang, “Improving the security of multiparty quantum secret sharing against trojan horse attack,” *Phys. Rev. A*, vol. 72, p. 044302, Oct 2005. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.72.044302>
- [3] Q.-Y. Cai, “Eavesdropping on the two-way quantum communication protocols with invisible photons,” *Physics Letters A*, vol. 351, no. 1, pp. 23 – 25, 2006. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0375960105016208>
- [4] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, “Improving the security of secure direct communication based on the secret transmitting order of particles,” *Phys. Rev. A*, vol. 74, p. 054302, Nov 2006. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.74.054302>

- [5] X.-B. Chen, G. Xu, X.-X. Niu, Q.-Y. Wen, and Y.-X. Yang, “An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement,” *Optics Communications*, vol. 283, no. 7, pp. 1561–1565, Apr. 2010. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0030401809012668>
- [6] W. Liu and Y.-B. Wang, “Quantum private comparison based on ghz entangled states,” *International Journal of Theoretical Physics*, vol. 51, no. 11, pp. 3596–3604, 2012. [Online]. Available: <http://dx.doi.org/10.1007/s10773-012-1246-z>
- [7] L. Wen, W. Yong-Bin, and C. Wei, “Quantum private comparison protocol based on bell entangled states,” *Communications in Theoretical Physics*, vol. 57, no. 4, pp. 583–, 2012. [Online]. Available: <http://stacks.iop.org/0253-6102/57/i=4/a=11>
- [8] W. Liu, Y.-B. Wang, and Z.-T. Jiang, “An efficient protocol for the quantum private comparison of equality with w state,” *Optics Communications*, vol. 284, no. 12, pp. 3160–3163, Jun. 2011. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0030401811001842>
- [9] W. Liu, Y.-B. Wang, Z.-T. Jiang, and Y.-Z. Cao, “A protocol for the quantum private comparison of equality with  $\sqrt{2}$ -type state,” *International Journal of Theoretical Physics*, vol. 51, no. 1, pp. 69–77, 2012. [Online]. Available: <http://dx.doi.org/10.1007/s10773-011-0878-8>
- [10] W. Liu, Y.-B. Wang, Z.-T. Jiang, Y.-Z. Cao, and W. Cui, “New quantum private comparison protocol using  $\sqrt{2}$ -type state,” *International Journal of Theoretical Physics*, vol. 51, no. 6, pp. 1953–1960, 2012. [Online]. Available: <http://dx.doi.org/10.1007/s10773-011-1073-7>

- [11] H.-Y. Tseng, J. Lin, and T. Hwang, “New quantum private comparison protocol using epr pairs,” *Quantum Information Processing*, vol. 11, no. 2, pp. 373–384, 2012. [Online]. Available: <http://dx.doi.org/10.1007/s11128-011-0251-0>
- [12] Y.-J. Chang, C.-W. Tsai, and T. Hwang, “Multi-user private comparison protocol using ghz class states,” *Quantum Information Processing*, vol. 12, no. 2, pp. 1077–1088, 2013. [Online]. Available: <http://dx.doi.org/10.1007/s11128-012-0454-z>
- [13] W. Liu, Y.-B. Wang, and X.-M. Wang, “Multi-party quantum private comparison protocol using d-dimensional basis states without entanglement swapping,” *International Journal of Theoretical Physics*, vol. 53, no. 4, pp. 1085–1091, 2014. [Online]. Available: <http://dx.doi.org/10.1007/s10773-013-1903-x>
- [14] W.-W. Zhang and K.-J. Zhang, “Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party,” *Quantum Information Processing*, vol. 12, no. 5, pp. 1981–1990, 2013. [Online]. Available: <http://dx.doi.org/10.1007/s11128-012-0507-3>
- [15] H.-K. Lo, “Insecurity of quantum secure computations,” *Phys. Rev. A*, vol. 56, no. 2, pp. 1154–1162, Aug. 1997. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevA.56.1154>
- [16] T. Hwang, Y.-P. Luo, C.-W. Yang, and T.-H. Lin, “Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants,” *Quantum Information Processing*, vol. 13, no. 4, pp. 925–933, 2014. [Online]. Available: <http://dx.doi.org/10.1007/s11128-013-0702-x>

- [17] Y.-P. Luo and T. Hwang, “Arbitrated quantum signature of classical messages without using authenticated classical channels,” *Quantum Information Processing*, vol. 13, no. 1, pp. 113–120, 2014. [Online]. Available: <http://dx.doi.org/10.1007/s11128-013-0634-5>
- [18] F. Gao, F.-Z. Guo, Q.-Y. Wen, and F.-C. Zhu, “Comment on “experimental demonstration of a quantum protocol for byzantine agreement and liar detection”,” *Phys. Rev. Lett.*, vol. 101, p. 208901, Nov 2008. [Online]. Available: <http://link.aps.org/doi/10.1103/PhysRevLett.101.208901>
- [19] G. Fei, L. Song, W. Qiao-Yan, and Z. Fu-Chen, “A special eavesdropping on one-sender versus n-receiver qsdcc protocol,” *Chinese Physics Letters*, vol. 25, no. 5, p. 1561, 2008. [Online]. Available: <http://stacks.iop.org/0256-307X/25/i=5/a=011>
- [20] F. Gao, S.-J. Qin, Q.-Y. Wen, and F.-C. Zhu, “A simple participant attack on the brádler-dušek protocol,” *Quantum Info. Comput.*, vol. 7, no. 4, pp. 329–334, May 2007. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2011725.2011729>